Offering Professional Offensive Security

BackTrack v2.0 – Developer notes for End Users

BackTrack Development Team

muts [at] remote-exploit [dot] org

BackTrack v2.0 – Developer notes for End Users

Greets:

Greets are usually reserved for the end. However, in this case, Backtrack would not be as it is without contributions made by the BackTrack community. I would like to thank Daniel Grimshaw aka Shadz from ethicalhacking.end0.net, for giving BackTrack the sleek look (sexy wallpaper, brilliant bootsplash, etc).

Notes:

Lots of thought and effort have been put into BT v2.0. My personal goal was to make myself an “OS replacement” - a distribution which could completely replace my Win XP base. This means that apart from the usual BackTrack tools - many day to day tools, such as gaim, skype, OpenOffice, vmware, calc (!), Tor, etc would be present, and 1 click away from me. Personally, I can say that I have reached my goal, and BT has replaced my default XP Installation. Windows is finally where it belongs...in a Virtual Machine, running over BT.

BackTrack was (and still is) in vigorous testing, and all (most?) of the small annoying bugs have been stomped out. Gaim supports SSL, Skype supports ALSA, ATI drivers are modularized, VMWare tools module seamlessly integrates into the image...you get the idea. We learned from all (most?) our mistakes in BT v1.0, and improved on the system in general.

What is Backtrack?

Backtrack Security Collection is a live CD system based on Slax. With no installation whatsoever, the security analysis platform is started directly from the CD-Rom / USB / Network or RAM and is fully accessible within minutes. Independent of the hardware in use, the Backtrack security collection offers a standardized security auditing working environment, so that the build-up of know-how and remote support is made easier. Even during the planning and development stages, our target was to achieve an excellent user-friendliness combined with an optimal array of tools. Professional open-source programs offer you a complete toolset to analyze your safety, byte for byte.

In order to become quickly proficient within the Backtrack security collection, the menu structure is supported by recognized phases of a security check. (foot-printing, analysis, scanning, wireless, brute-forcing, cracking). By this means, you intuitively find the right tool for the appropriate task. In addition to the approximately 300 tools, the Backtrack security collection contains a working environment for complex tools and setups, such as Snort, ntop, db_autopwn, kismet with gps support, kismet autoconfiguration , unicornscan pgsql support and other nifty features.

Current productivity tools such as web browser, editors and graphic tools allow you to create or edit texts and pictures for reports, directly within the Backtrack security platform. Many tools were adapted, newly developed or converted from other system platforms, in order to make as many current auditing tools available as possible on one CD-ROM.

New BackTrack v2.0 features:

Updated Kernel – Running 2.6.18-rc5, with several patches.

- Kernel has been updated, and patched with lots of stuff. Much better hardware support, and much more stable than BT v1.0. A wider range of wireless cards is supported, and better support for dual core systems (even though still problematic).

Updated Tools – Old versions updated, new tools added.

- Old tools updated, new tools added. Special attention was given to tools like Metasploit db_autopwn, Unicornscan pgsqldb and others, which demand all sorts of weird dependencies and libs.

BackTrack Network Boot – Boot additional BackTrack images over PXE

- A wonderful new feature that allows to boot up additional BackTrack machines over the network, using PXE enabled NICs. This is especially useful in a classroom situation, where you need a simple and quick way to distribute BT to a large amount of people, instantly. This feature is not released in the beta.

John MPI instant Cluster – Boot BackTrack cracking cluster clients over PXE

- Same idea as above, except that smaller footprint clients can be booted into a cracking cluster, using JRT MPI. This feature is not released in the beta, and will have a separate article describing usage.

Save2CD – Save changes to CD (assuming CD is multi-session, and a CDR).

- An exciting new feature that allows to save changes directly to CD. The prerequisites for this are a CDR, and BT burnt onto a CD, with multi session support (In Nero, clear the “No further writing possible” and choose “Disk at Once”).

Japanese Input Support – Reading and writing in Hiragana / Katakana / Kanji.

- Japanese / Chinese fonts integrated into the base BT image. Special effort was put to enable Japanese Input (writing Kanji, Hiragana and Katakana) – using scim and anthy. Thanks to #Japan on efnet !

Unionfs replaced – by aufs with zlib compression.

- Zlib compression allows for smaller mo's (more apps crammed into BT, however disk operations such as dir2mo take longer, and more processor intensive). This also means that BT v2.0 modules are not compatible with v.1.0 or with old SLAX modules.

Kernel Sources – Included in base image. No more "where is kernel.mo ?".

- The replacement of unionfs to aufs allowed for more megabytes to be packed into the ISO. We decided to include the kernel sources with this distribution, for maximum customization and minimum hassle.

Special Features:

- **Instant Snort Setup** – Sets up snort, mysql, apache, base (/usr/bin/setup-snort).
- **Instant db_autopwn Setup** – Sets up Pgsql for Metasploit3.
- **Instant Unicornscan pgsqldb Setup** - Sets up Apache, Pgsql for scan info.
- **Kismet auto configuration** – Sets up monitor mode and kismet.conf.
- **ipw3945/2200/2100 support** – no injection patches! (get a real card).
- **Prism54 / MadWifi-ng / Wlan-ng / HostAP / rt2570** – With injection patches.
- **Quick Installation** – Using GUI installer, 100% MySlax compatible.

Useful commands:

- **ati** – initializes the ATI Xconf and starts KDE.
- **startx** – starts KDE.
- **flux** – starts Fluxbox.
- **share** – mounts a windows share to /mnt/share.
- **leetmode** – starts a KDE Sensor array (karamba) .
- **start-kismet-ng** – auto configures kismet.conf and runs kismet.
- **fixvesa** – restore original vesa xconf (not in beta).
- **sshd-generate** – creates SSH Keys. Usually followed by /usr/sbin/sshd.

Cheat Codes:

You can customize the boot process, by supplying different boot parameters. You can check the slax.org site for the Slax based codes available. Here are some BT specific codes :

- **bt** – default boot.
- **dbt** – dual core support (default boot has dual core disabled).
- **safe** – loads BT with a failsafe configuration.
- **debug** – load BT in DEBUG mode.
- **client** – PXE boot cracking client (not in beta).
- **server** – PXE boot cracking server (not in beta).

Optional Modules:

You can load optional modules at boot time, depending on your needs - eg:
load=ati (use this if you have a Notebook with an ATI video card).
load=vmware-tools|pxe|server (will load all 3 optional modules).

Making Modules:

If you have a piece of software you would like to see included in Backtrack or if you would like to make an addition to Backtrack, then you need to submit a module. Modules are, directories and or files bundled into a format that makes it easy for the Backtrack Development Team to include. All modules should be submitted to muts@remote-exploit.org.

Source code:

Since BackTrack is based on SLAX, the method for creating modules is the same. A simple example using amap 5.2:

```
BT:~# cd /tmp
BT tmp # mkdir /MODULES/pentest/scanners
BT tmp # cd /MODULES/pentest/scanners
BT tmp # wget http://thc.org/releases/amap-5.2.tar.gz
--11:07:09--  http://thc.org/releases/amap-5.2.tar.gz
           => `amap-5.2.tar.gz'
Resolving thc.org... 82.165.25.125
Connecting to thc.org|82.165.25.125|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 262,875 (257K) [application/x-tar]

100%[====================================>] 262,875       68.45K/s    ETA 00:00

11:07:15 (68.30 KB/s) - `amap-5.2.tar.gz' saved [262875/262875]

BT:~# tar zxpf amap-5.2.tar.gz
BT:~# cd amap-5.2
BT amap-5.2 # ./configure && make
BT amap-5.2 # checkinstall
The package documentation directory ./doc-pak does not exist.
Should I create a default set of package docs?  [y]: n

Please choose the packaging method you want to use.
Slackware [S], RPM [R] or Debian [D]? S

Please write a description for the package. Remember that pkgtool shows
```

```
only the first one when listing packages so make that one descriptive.

End your description with an empty line or EOF.
>> Amap 5.2


>>

*********************************************
**** Slackware package creation selected ***
*********************************************


This package will be built according to these values:

1 -  Summary: [ Amap 5.2 ]
2 -  Name:    [ amap ]
3 -  Version: [ 5.2 ]
4 -  Release: [ 1 ]
5 -  License: [ GPL ]
6 -  Group:   [ Applications/System ]
7 -  Architecture: [ i386 ]
8 -  Source location: [ amap-5.2 ]
9 -  Alternate source location: [  ]
10 - Requires: [  ]

Enter a number to change any of them or press ENTER to continue:

BT amap-5.2 #
BT amap-5.2 # tgz2mo amap-5.2-i386-1.tgz amap-5.2.mo
Installing package amap-5.2-i386-1...
PACKAGE DESCRIPTION:
amap: Amap 5.2
Executing install script for amap-5.2-i386-1...

BT amap-5.2 #
```

Directory Structure:

Creating the modules can be a little tricky since the files can end up in the wrong place. Now, if you wanted to add a binary or configuration file to the /pentest/cisco folder you would do the following:

```
BT:~# mkdir -p /tmp/MODULES/pentest/cisco
```

Copy the binaries and files you want into /tmp/MODULES/pentest/cisco
(If you plan on adding to the directory copy the current contents of /pentest/cisco, or any folder other folder that you are adding files, into your new folder)

```
BT:~# cd /tmp
BT tmp # dir2mo MODULES pentest-cisco.mo
```

This method insures the mo will be extracted into /pentest/cisco properly.

What is Snort?

Snort® is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. With millions of downloads to date, Snort is the most widely deployed intrusion detection and prevention technology worldwide and has become the de facto standard for the industry. (www.snort.org)

How do I setup Snort?

The easy installation process for Snort has been incorporated into Backtrack. Therefore, setting it up is just a few simple steps.

```
BT:~# setup-snort
```

Then simply following the instructions.

Direct your web browser at:
http://IP-BACKTRACK/base/base_db_setup.php

1) Click Create BASE AG on the far right side
2) Click Main Page link above Alert Group Maintenance

Known Issues:

Q. On boot, I get ***-> aufs test_add:305:exe[2121]: different uid/gid/permission***.
A. That's normal, stop whining.

Q. My atheros does not work!
A. BT uses madwifi-ng. Try ***airmon-ng start wifi0***, and use **ath1** for attacks.

Q. My ATI radon card does not work!
A. Include the ati.mo, and when in console, type **ati**.

Q. My ATI radon card still does not work!
A. Pray to the driver gods and hope ATI come up with fixes.

Q. Where is tool X?
A. There are a few possibilities. First, it is possible that the tool is installed in somewhere under the /pentest directory. You will need to change to the proper directory to execute it. The other possibility is that it isn't installed. If a tool is missing, we recommend that you take it as your call to action and create a module for us to include. Follow the step listed above in the Making Modules section.

Q. I still have questions where can I go for help?

A. There are plenty of places you can go for more help regarding issues with Backtrack. The first place to go is to the website http://www.remote-exploit.org. From the website you will see a link to the web-forum where many people's questions are already answered. The forum should be your first place to seek help. Next, search the website and the FAQ which contains solutions tocommon problems. The next location you should go is Google. If all of those don't have the answer there is an IRC channel on irc.freenode.net the channel is #remote-exploit where many users and developers hang out. A note of caution though, make sure you have looked around the website, the forum and checked Google before posting a question.